HPE6-A84$^{\text{Q\&As}}$

Aruba Certified Network Security Expert Written

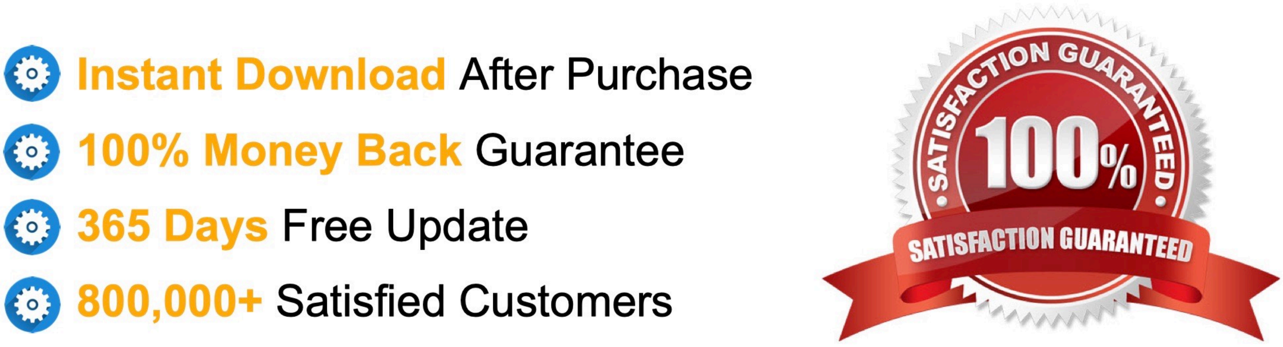
Pass HP HPE6-A84 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/hpe6-a84.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

1.

Permitted to receive IP addresses with DHCP

2.

Permitted access to DNS services from 10.8.9.7 and no other server

3.

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

4.

Denied access to other 10.0.0.0/8 subnets

5.

Permitted access to the Internet

6.

Denied access to the WLAN for a period of time if they send any SSH traffic

7.

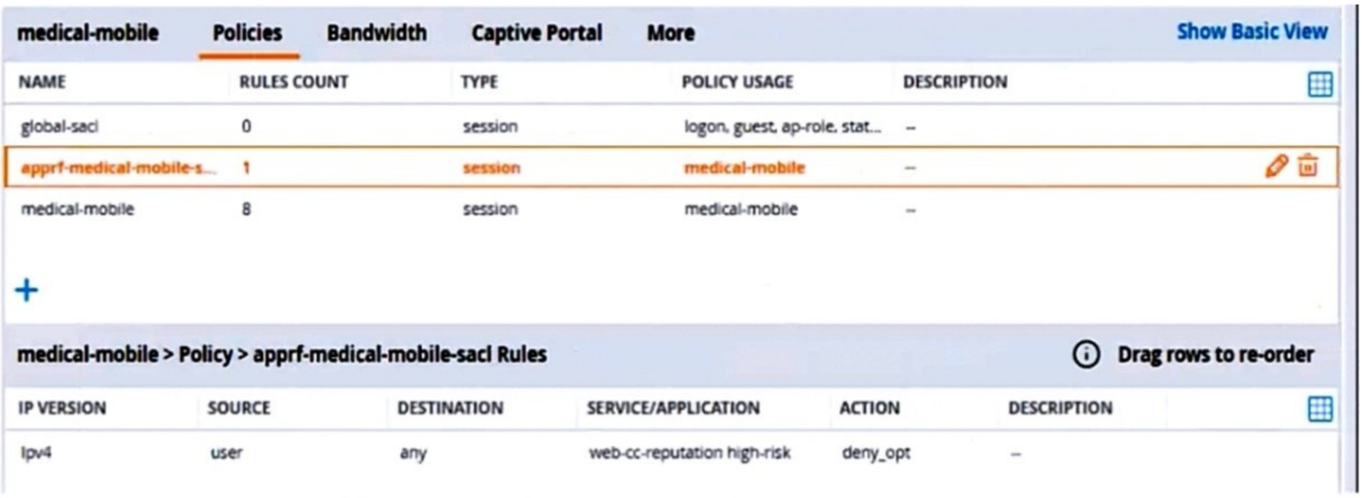
Denied access to the WLAN for a period of time if they send any Telnet traffic

8.

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

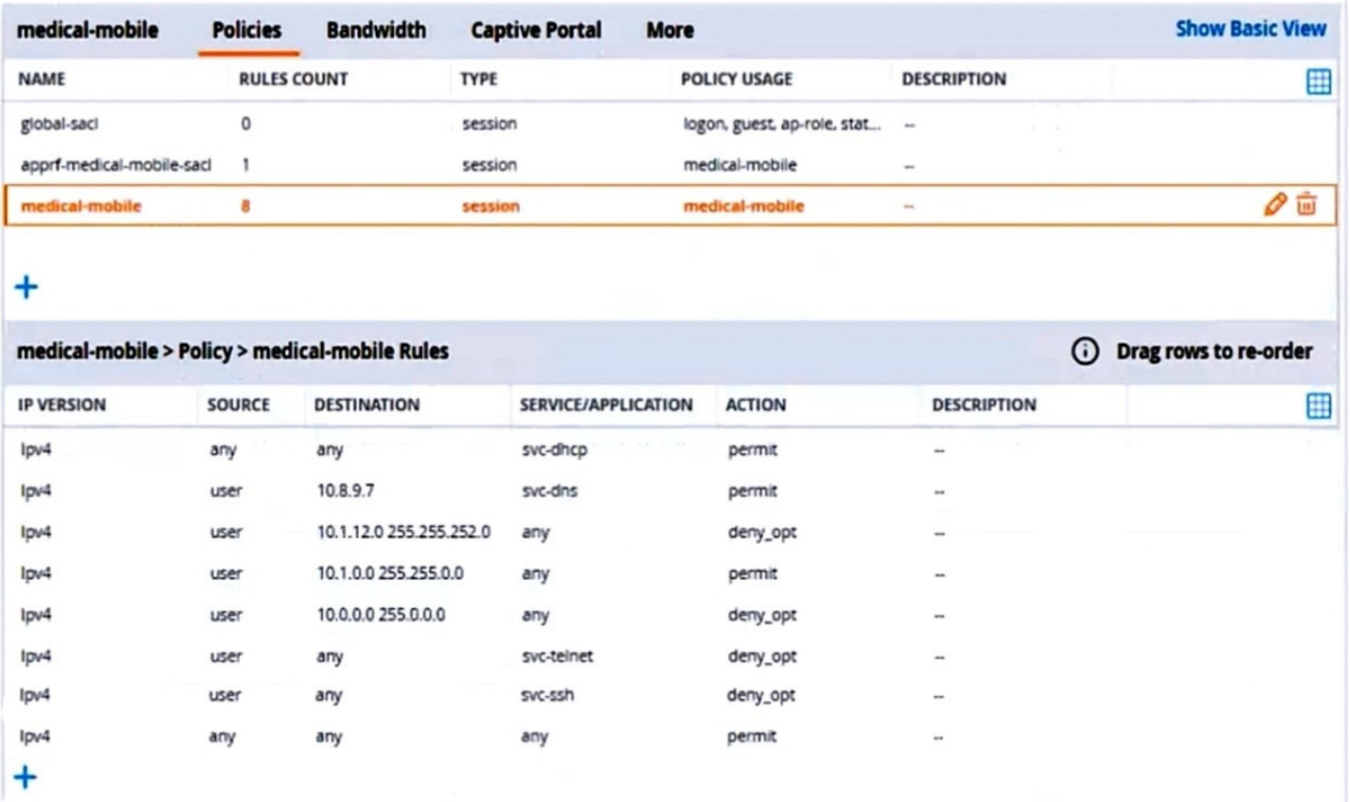
The exhibits below show the configuration for the role.



NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

medical-mobile > Policy > apprf-medical-mobile-sacl Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
Ipv4	user	any	web-cc-reputation high-risk	deny_opt	--



NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-sacl	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

medical-mobile > Policy > medical-mobile Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
Ipv4	any	any	svc-dhcp	permit	--
Ipv4	user	10.8.9.7	svc-dns	permit	--
Ipv4	user	10.1.12.0 255.255.252.0	any	deny_opt	--
Ipv4	user	10.1.0.0 255.255.0.0	any	permit	--
Ipv4	user	10.0.0.0 255.0.0.0	any	deny_opt	--
Ipv4	user	any	svc-telnet	deny_opt	--
Ipv4	user	any	svc-ssh	deny_opt	--
Ipv4	any	any	any	permit	--

There are multiple issues with the configuration.

What is one of the changes that you must make to the policies to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, "medical-mobile" rule 1 is "ipv4 any any svc-dhcp permit," and rule 8 is "ipv4 any any any permit\\'.)

A. In the "medical-mobile" policy, change the source in rule 1 to "user."

B. In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.

C. In the "medical-mobile" policy, move rules 6 and 7 to the top of the list.

D. Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.

Correct Answer: C

Rules 6 and 7 in the "medical-mobile" policy are used to deny access to the WLAN for a period of time if the clients send any SSH or Telnet traffic, as required by the scenario. However, these rules are currently placed below rule 5, which permits access to the Internet for any traffic. This means that rule 5 will override rules 6 and 7, and the clients will not be denied access to the WLAN even if they send SSH or Telnet traffic. To fix this issue, rules 6 and 7 should be moved to the top of the list, before rule 5. This way, rules 6 and 7 will take precedence over rule 5, and the clients will be denied access to the WLAN if they send SSH or Telnet traffic, as expected.

QUESTION 2

You want to use Device Insight tags as conditions within CPPM role mapping or enforcement policy rules.

What guidelines should you follow?

A. Create an HTTP authentication source to the Central API that queries for the tags. To use that source as the type for rule conditions, add it an authorization source for the service in question.

B. Use the Application type for the rule conditions; no extra authorization source is required for services that use policies with these rules.

C. Use the Endpoints Repository type for the rule conditions; Add Endpoints Repository as a secondary authentication source for services that use policies with these rules.

D. Use the Endpoint type for the rule conditions; no extra authorization source is required for services that use policies with these rules.

Correct Answer: D

According to the Aruba Cloud Authentication and Policy Overview1, Device Insight tags are stored in the Endpoint Repository and can be used as conditions within CPPM role mapping or enforcement policy rules. The rule condition type should be Endpoint, and the attribute should be Device Insight Tags. No extra authorization source is required for services that use policies with these rules. Therefore, option D is the correct answer. Option A is incorrect because creating an HTTP authentication source to the Central API is not necessary to use Device Insight tags as conditions. Device Insight tags are already synchronized between Central and CPPM, and can be accessed from the Endpoint Repository. Option B is incorrect because using the Application type for the rule conditions is not applicable to Device Insight tags. The Application type is used to match attributes from the Application Authentication source, which is used to integrate with third-party applications such as Microsoft Intune or Google G Suite. Option C is incorrect because using the Endpoints Repository type for the rule conditions is not valid for Device Insight tags. The Endpoints Repository type is used to match attributes from the Endpoints Repository source, which is different from the Endpoint type. The Endpoints Repository source contains information about endpoints that are manually added or imported into CPPM, while the Endpoint type contains information about endpoints that are dynamically discovered and profiled by CPPM or Device Insight. Adding Endpoints Repository as a secondary authentication source for services that use policies with these rules is also unnecessary and redundant.

QUESTION 3

Refer to the scenario.

An organization wants the AOS-CX switch to trigger an alert if its RADIUS server (cp.acnsxtest.local) rejects an unusual number of client authentication requests per hour. After some discussions with other Aruba admins, you are still not sure how many rejections are usual or unusual. You expect that the value could be different on each switch. You are helping the developer understand how to develop an NAE script for this use case.

The developer explains that they plan to define the rule with logic like this:

monitor > value

However, the developer asks you what value to include.

What should you recommend?

A. Checking one of the access switches\\' RADIUS statistics and adding 10 to the number listed for rejects

B. Defining a baseline and referring to it for the value

C. Using 10 (per hour) as a good starting point for the value

D. Defining a parameter and referring to it (self ^ramsfname]) for the value

Correct Answer: D

This is because a parameter is a variable that can be defined and modified by the user or the script, and can be used to customize the behavior and output of the NAE script. A parameter can be referred to by using the syntax self ^ramsfname], where ramsfname is the name of the parameter. By defining a parameter for the value, the developer can make the NAE script more flexible and adaptable to different scenarios and switches. The parameter can be set to a default value, such as 10, but it can also be changed by the user or the script based on the network conditions and requirements. For example, the parameter can be adjusted dynamically based on the average or standard deviation of the number of rejects per hour, or based on the feedback from the user or other admins. This way, the NAE script can trigger an alert only when the number of rejects is truly unusual and not just arbitrary. A. Checking one of the access switches\\' RADIUS statistics and adding 10 to the number listed for rejects. This is not a good recommendation because it does not account for the variability and diversity of the network environment and switches. The number of rejects listed for one switch might not be representative or relevant for another switch, as different switches might have different traffic patterns, client types, RADIUS configurations, etc. Moreover, adding 10 to the number of rejects is an arbitrary and fixed value that might not reflect the actual threshold for triggering an alert. B. Defining a baseline and referring to it for the value. This is not a bad recommendation, but it is not as good as defining a parameter. A baseline is a reference point that represents the normal or expected state of a network metric or performance indicator. A baseline can be used to compare and contrast the current network situation and detect any anomalies or deviations. However, a baseline might not be easy or accurate to define, as it might require historical data, statistical analysis, or expert judgment. Moreover, a baseline might not be stable or constant, as it might change over time due to network growth, evolution, or optimization.

C. Using 10 (per hour) as a good starting point for the value. This is not a good recommendation because it is an arbitrary and fixed value that might not reflect the actual threshold for triggering an alert. Using 10 (per hour) as the value might result in false positives or false negatives, depending on the network conditions and switches. For example, if the normal number of rejects per hour is 5, then using 10 as the value might trigger an alert too frequently and unnecessarily. On the other hand, if the normal number of rejects per hour is 15, then using 10 as the value might miss some important alerts and risks.

QUESTION 4

Refer to the scenario.

A customer has an AOS10 architecture that is managed by Aruba Central. Aruba infrastructure devices authenticate clients to an Aruba ClearPass cluster.

In Aruba Central, you are examining network traffic flows on a wireless IoT device that is categorized as "Raspberry Pi" clients. You see SSH traffic. You then check several more wireless IoT clients and see that they are sending SSH also.

You want an easy way to communicate the information that an IoT client has used SSH to Aruba ClearPass Policy Manager (CPPM).

What step should you take?

A. On CPPM create an Endpoint Context Server that points to the Central API.

B. On CPPM enable Device Insight integration.

C. On Central configure APs and gateways to use CPPM as the RADIUS accounting server.

D. On Central set up CPPM as a Webhook application.

Correct Answer: A

This is because an Endpoint Context Server (ECS) is a feature that allows ClearPass to receive contextual information from external sources, such as Aruba Central, and use it for policy enforcement and reporting. An ECS can be configured to point to the Aruba Central API and fetch data such as device type, category, OS, applications, traffic flows, etc. An ECS can be used to communicate the information that an IoT client has used SSH to Aruba ClearPass Policy Manager (CPPM). The ECS can query the Aruba Central API and retrieve the network traffic flows of the wireless IoT devices that are categorized as "Raspberry Pi" clients. The ECS can then filter the traffic flows by the SSH protocol and send the relevant information to CPPM. CPPM can then use this information for policy decisions, such as allowing or denying SSH access, or triggering alerts or actions. B. On CPPM enable Device Insight integration. This is not a valid step because Device Insight is a feature that allows ClearPass to discover, profile, and fingerprint devices on the network using deep packet inspection (DPI) and machine learning (ML). Device Insight does not communicate with Aruba Central or receive information from it. Moreover, Device Insight might not be able to detect SSH traffic on encrypted wireless IoT devices without decrypting it first.

C. On Central configure APs and gateways to use CPPM as the RADIUS accounting server. This is not a valid step because RADIUS accounting is a feature that allows network devices to send periodic updates about the status and activity of authenticated users or devices to a RADIUS server, such as CPPM. RADIUS accounting does not communicate with Aruba Central or receive information from it. Moreover, RADIUS accounting might not be able to capture SSH traffic on wireless IoT devices without inspecting it first.

D. On Central set up CPPM as a Webhook application. This is not a valid step because Webhook is a feature that allows Aruba Central to send notifications or events to external applications or services using HTTP requests. Webhook does not communicate with CPPM or send information to it. Moreover, Webhook might not be able to send SSH traffic information on wireless IoT devices without filtering it first.

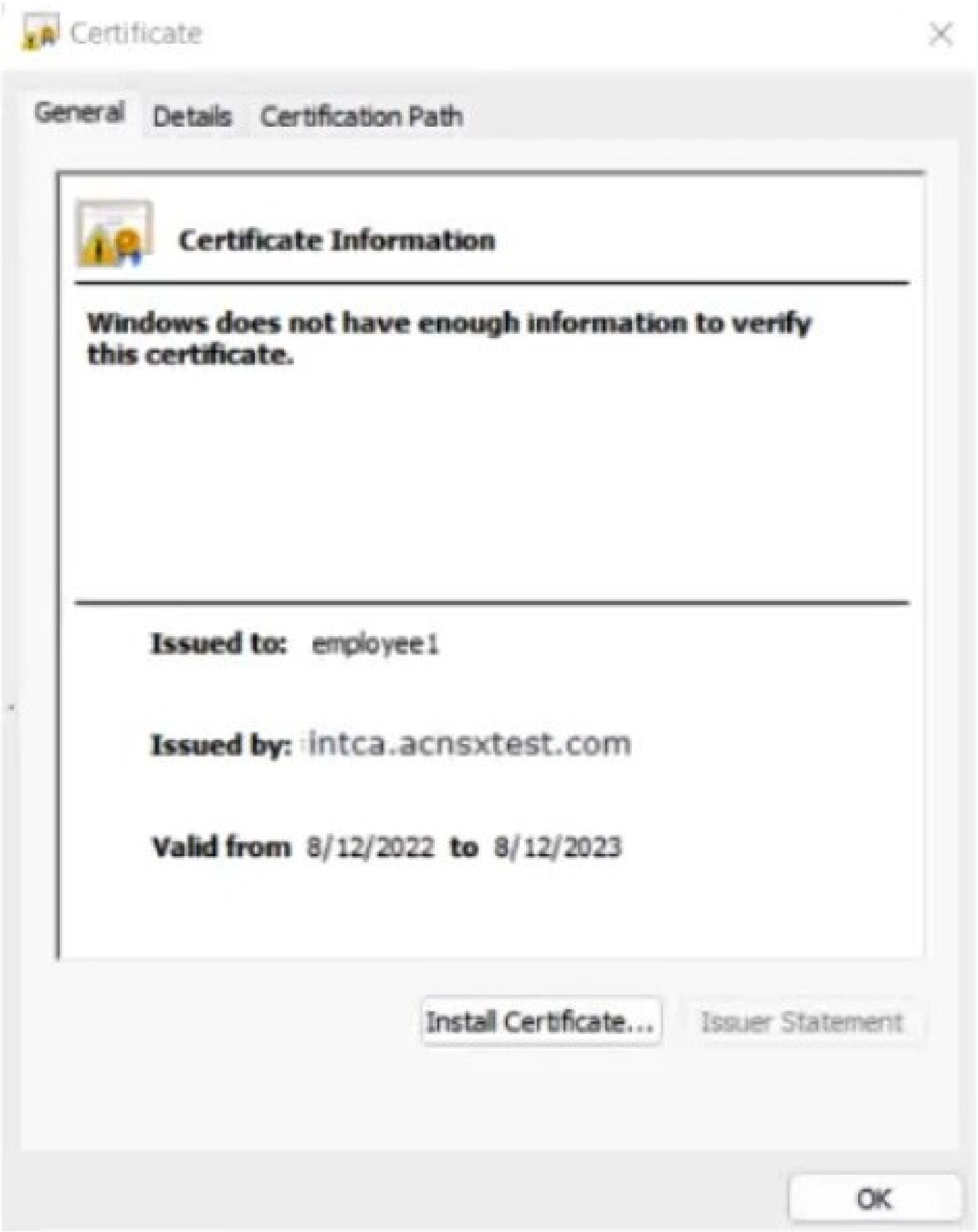
QUESTION 5

Refer to the scenario.

# Introduction to the customer

You are helping a company add Aruba ClearPass to their network, which uses Aruba network infrastructure devices.

The company currently has a Windows domain and Windows CA. The Window CA issues certificates to domain computers, domain users, and servers such as domain controllers. An example of a certificate issued by the Windows CA is shown here.

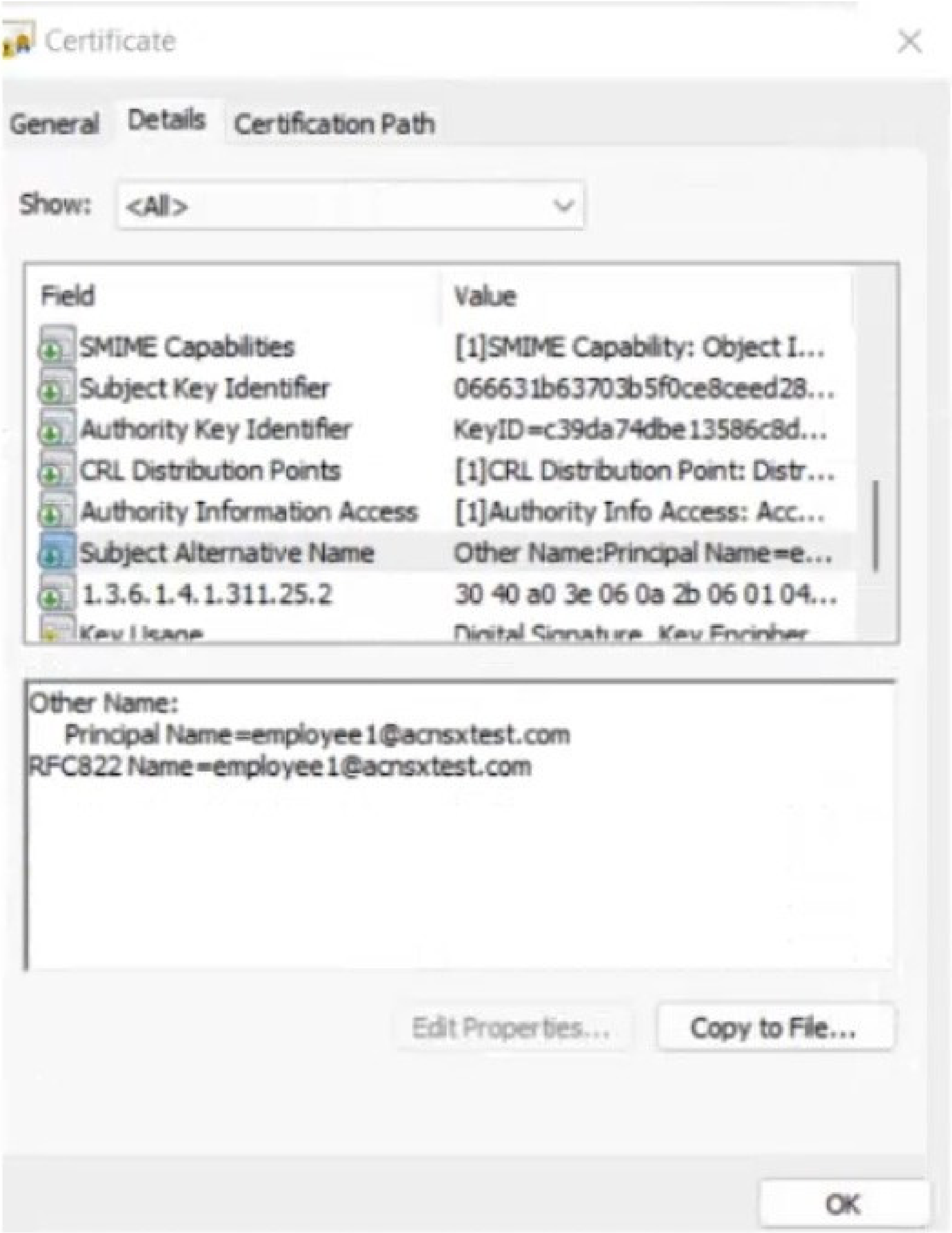


Windows does not have enough information to verify this certificate.

Issued to: employee1

Issued by: intca.acnsxtest.com

Valid from 8/12/2022 to 8/12/2023



Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	066631b63703b5f0ce8ceed28...
Authority Key Identifier	KeyID=c39da74dbe13586c8d...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=e...
1.3.6.1.4.1.311.25.2	30 40 a0 3e 06 0a 2b 06 01 04...
Key Usage	Digital Signature, Key Encipher

Other Name:
Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com

The company is in the process of adding Microsoft Endpoint Manager (Intune) to manage its mobile clients. The customer is maintaining the on-prem AD for now and uses Azure AD Connect to sync with Azure AD.

# Requirements for issuing certificates to mobile clients

The company wants to use ClearPass Onboard to deploy certificates automatically to mobile clients enrolled in Intune. During this process, Onboard should communicate with Azure AD to validate the clients. High availability should also be

provided for this scenario; in other words, clients should be able to get certificates from Subscriber 2 if Subscriber 1 is down.

The Intune admins intend to create certificate profiles that include a UPN SAN with the UPN of the user who enrolled the device.

# Requirements for authenticating clients

The customer requires all types of clients to connect and authenticate on the same corporate SSID.

The company wants CPPM to use these authentication methods:

1.

EAP-TLS to authenticate users on mobile clients registered in Intune

2.

TEAR, with EAP-TLS as the inner method to authenticate Windows domain computers and the users on them To succeed, EAP-TLS (standalone or as a TEAP method) clients must meet these requirements:

1.

Their certificate is valid and is not revoked, as validated by OCSP

2.

The client\\'s username matches an account in AD # Requirements for assigning clients to roles After authentication, the customer wants the CPPM to assign clients to ClearPass roles based on the following rules:

1.

Clients with certificates issued by Onboard are assigned the "mobile-onboarded" role

2.

Clients that have passed TEAP Method 1 are assigned the "domain-computer" role

3.

Clients in the AD group "Medical" are assigned the "medical-staff" role

4.

Clients in the AD group "Reception" are assigned to the "reception-staff" role The customer requires CPPM to assign authenticated clients to AOS firewall roles as follows:

1.

Assign medical staff on mobile-onboarded clients to the "medical-mobile" firewall role

2.

Assign other mobile-onboarded clients to the "mobile-other" firewall role

3.

Assign medical staff on domain computers to the "medical-domain" firewall role

4.

All reception staff on domain computers to the "reception-domain" firewall role

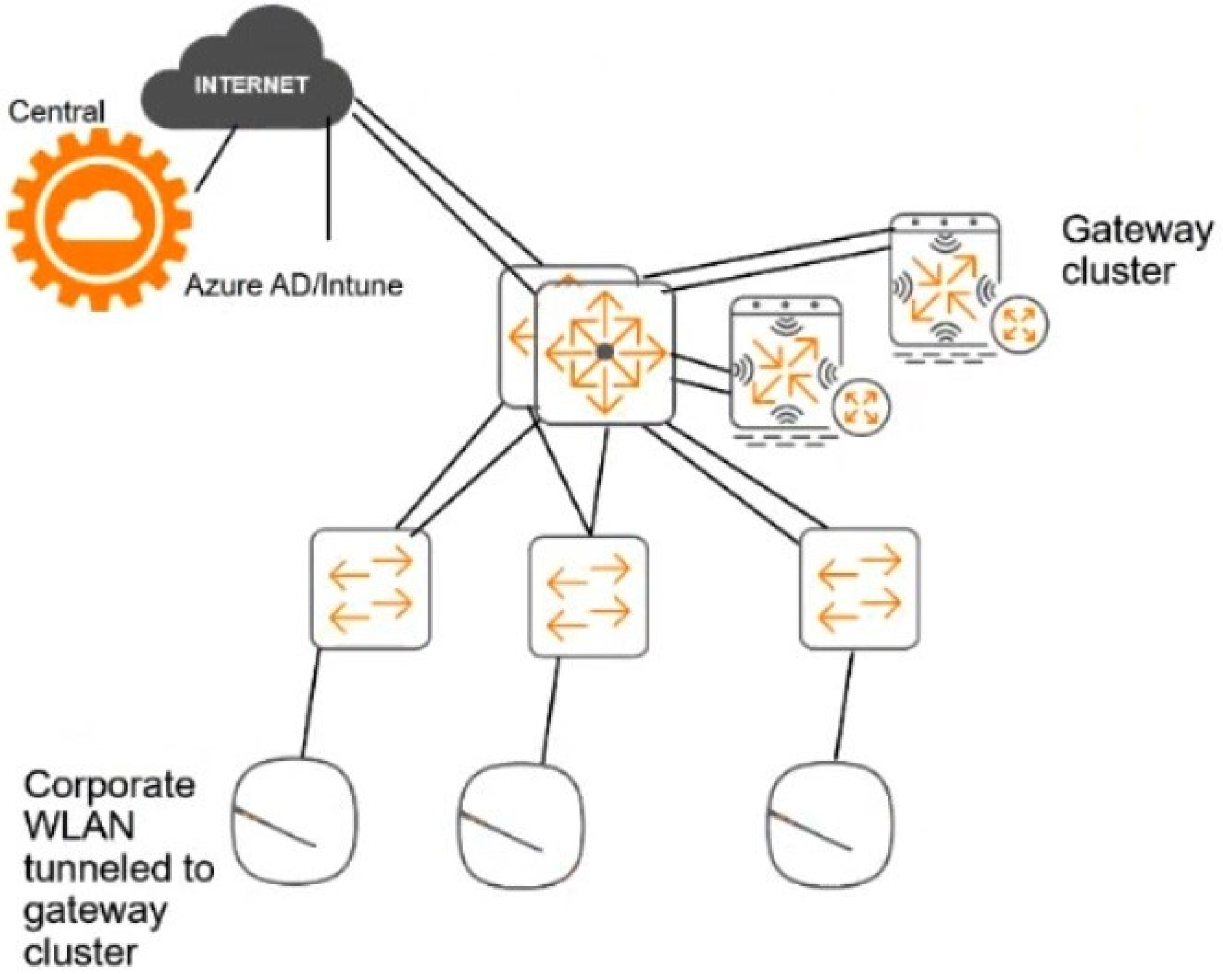
5.

All domain computers with no valid user logged in to the "computer-only" firewall role

6.

Deny other clients access # Other requirements Communications between ClearPass servers and on-prem AD domain controllers must be encrypted. # Network topology For the network infrastructure, this customer has Aruba APs and Aruba gateways, which are managed by Central. APs use tunneled WLANs, which tunnel traffic to the gateway cluster. The customer also has AOS-CX switches that are not

managed by Central at this point.



# ClearPass cluster IP addressing and hostnames A customer\\'s ClearPass cluster has these IP addresses:

1.

Publisher = 10.47.47.5

2.

Subscriber 1 = 10.47.47.6

3.

Subscriber 2 = 10.47.47.7

4.

Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8

The customer\\'s DNS server has these entries

1.

cp.acnsxtest.com = 10.47.47.5

2.

cps1.acnsxtest.com = 10.47.47.6

3.

cps2.acnsxtest.com = 10.47.47.7

4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

You have imported the root certificate for the Windows CA to the ClearPass CA Trust list.

Which usages should you add to it based on the scenario requirements?

A. EAP and AD/LDAP Server

B. LDAP and Aruba infrastructure

C. Radsec and Aruba infrastructure

D. EAP and Radsec

Correct Answer: A

QUESTION 6

A company has Aruba gateways that are Implementing gateway IDS/IPS in IDS mode. The customer complains that admins are receiving too frequent of repeat email notifications for the same threat. The threat itself might be one that the admins should investigate, but the customer does not want the email notification to repeat as often.

Which setting should you adjust in Aruba Central?

A. Report scheduling settings

B. Alert duration and threshold settings

C. The IDS policy setting (strict, medium, or lenient)

D. The allowlist settings in the IDS policy

Correct Answer: B

Alert duration and threshold settings are used to control how often and under what conditions email notifications are sent for gateway IDS/IPS events 1. By adjusting these settings, the customer can reduce the frequency of repeat email

notifications for the same threat, while still being informed of any critical or new threats. To adjust the alert duration and threshold settings in Aruba Central, the customer can follow these steps 1:

In the Aruba Central app, set the filter to Global, a group, or a device.

Under Analyze, click Alerts and Events.

Click the Config icon to open the Alert Severities and Notifications page. Select the Gateway IDS/IPS tab to view the alert categories and severities for gateway IDS/IPS events.

Click on an alert category to expand it and view the alert duration and threshold settings for each severity level.

Enter a value in minutes for the alert duration. This is the time period during which the alert is active and email notifications are sent. Enter a value for the alert threshold. This is the number of times the alert must be triggered within the alert

duration before an email notification is sent.

Click Save.

By increasing the alert duration and/or threshold values, the customer can reduce the number of email notifications for recurring threats, as they will only be sent when the threshold is reached within the duration. For example, if the customer sets the alert duration to 60 minutes and the alert threshold to 10 for a Critical severity level, then an email notification will only be sent if the same threat occurs 10 times or more within an hour.

QUESTION 7

Which element helps to lay the foundation for solid network security forensics?

A. Enable BPDU protection and loop protection on edqe switch ports

B. Enabling debug-level information for network infrastructure device logs

C. Implementing 802.1X authentication on switch ports that connect to APs

D. Ensuring that all network devices use a correct, consistent clock

Correct Answer: D

This is because network forensics relies on the analysis of network traffic data, which is often time-stamped by the devices that generate or transmit it. Having a synchronized and accurate clock across all network devices helps to establish a reliable timeline of events and correlate different sources of evidence12 A. Enable BPDU protection and loop protection on edge switch ports is not related to network security forensics, but rather to preventing network loops and topology changes caused by rogue switches or bridges3

B. Enabling debug-level information for network infrastructure device logs might provide more details about the network activity, but it also consumes more resources and storage, and might not be relevant or useful for forensic analysis. Moreover, debug-level information might not be available for long-term retention or legal purposes4 C. Implementing 802.1X authentication on switch ports that connect to APs is a good security practice to prevent unauthorized access to the network, but it does not directly help with network security forensics. 802.1X authentication does not capture or record network traffic data, which is the main source of evidence for network forensics

QUESTION 8

You are working with a developer to design a custom NAE script for a customer. The NAE agent should trigger an alert when ARP inspection drops packets on a VLAN. The customer wants the admins to be able to select the correct VLAN ID for the agent to monitor when they create the agent.

What should you tell the developer to do?

A. Use this variable, %{vlan-id} when defining the monitor URI in the NAE agent script.

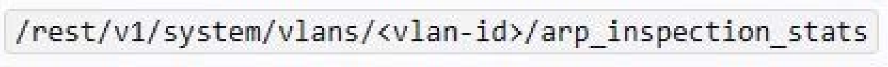
B. Define a VLAN ID parameter; reference that parameter when defining the monitor URI.

C. Create multiple monitors within the script from which admins can select when they create the agent.

D. Use a callback action to collect the ID of the VLAN on which admins have enabled NAE monitoring.

Correct Answer: B

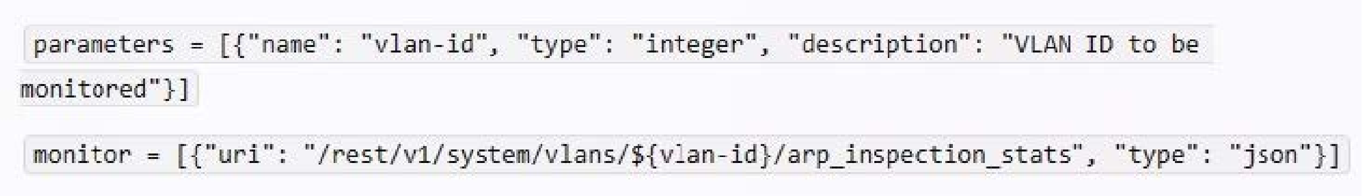
A custom NAE script is a Python script that defines the monitors, the alert-trigger logic, and the remedial actions for an NAE agent. A monitor is a URI that specifies the data source and the data type that the NAE agent should collect and analyze. For example, to monitor the ARP inspection statistics on a VLAN, the monitor URI would be something like this:



```
/rest/v1/system/vlans/<vlan-id>/arp_inspection_stats
```

where is the ID of the VLAN to be monitored.

To allow the admins to select the correct VLAN ID for the agent to monitor when they create the agent, you need to define a VLAN ID parameter in the NAE script. A parameter is a variable that can be set by the user when creating or modifying an agent. A parameter can be referenced in other parts of the script by using the syntax ${parameter-name}. For example, to define a VLAN ID parameter and reference it in the monitor URI, you would write something like this: This way, when the admins create or modify the agent, they can enter the VLAN ID that they want to monitor, and the NAE script will use that value in the monitor URI. You can find more information about how to write custom NAE scripts and use parameters in the NAE Scripting Guide



```
parameters = [{"name": "vlan-id", "type": "integer", "description": "VLAN ID to be
monitored"}]

monitor = [{"uri": "/rest/v1/system/vlans/${vlan-id}/arp_inspection_stats", "type": "json"}]
```

QUESTION 9

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients\\' privileges, ClearPass also should use information collected by Intune to make access control decisions.

Assume that the Azure AD deployment has the proper prerequisites established.

You are planning the CPPM authentication source that you will reference as the authentication source in 802.1X services.

How should you set up this authentication source?

A. As Kerberos type

B. As Active Directory type

C. As HTTP type, referencing the Intune extension

D. AS HTTP type, referencing Azure AD\\'s FODN

Correct Answer: D

An authentication source is a configuration element in CPPM that defines how to connect to an external identity provider and retrieve user or device information . CPPM supports various types of authentication sources, such as Active

Directory, LDAP, SQL, Kerberos, and HTTP .

To authenticate wireless and wired clients to Azure AD, you need to set up an authentication source as HTTP type, referencing Azure AD\\'s FQDN . This type of authentication source allows CPPM to use REST API calls to communicate with

Azure AD and validate the user or device credentials . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

To use information collected by Intune to make access control decisions, you need to set up another authentication source as HTTP type, referencing the Intune extension . This type of authentication source allows CPPM to use REST API

calls to communicate with Intune and retrieve the device compliance status . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

QUESTION 10

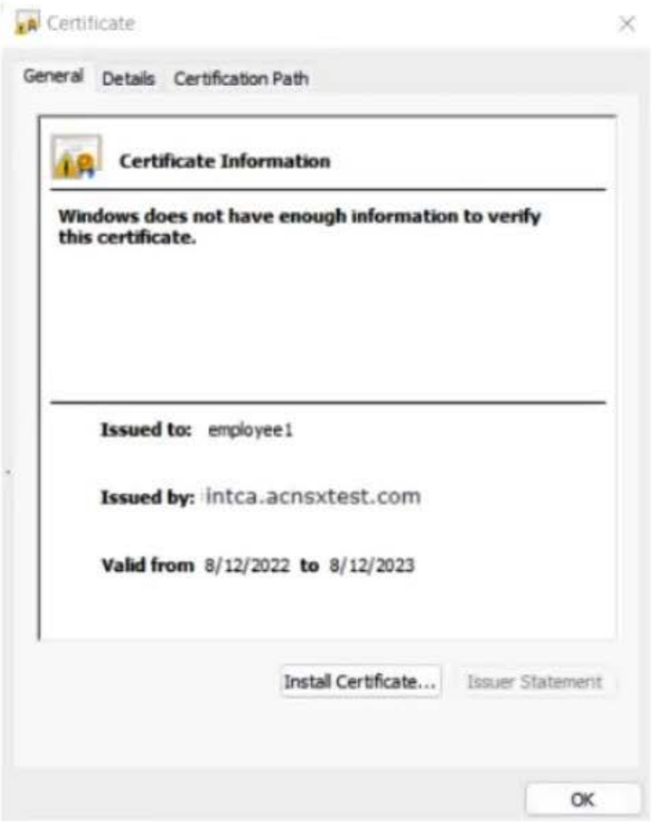
Refer to the scenario.

Introduction to the customer

You are helping a company add Aruba ClearPass to their network, which uses Aruba network infrastructure devices.

The company currently has a Windows domain and Windows CA. The Window CA issues certificates to domain computers, domain users, and servers such as domain controllers. An example of a certificate issued by the Windows CA is

shown here.



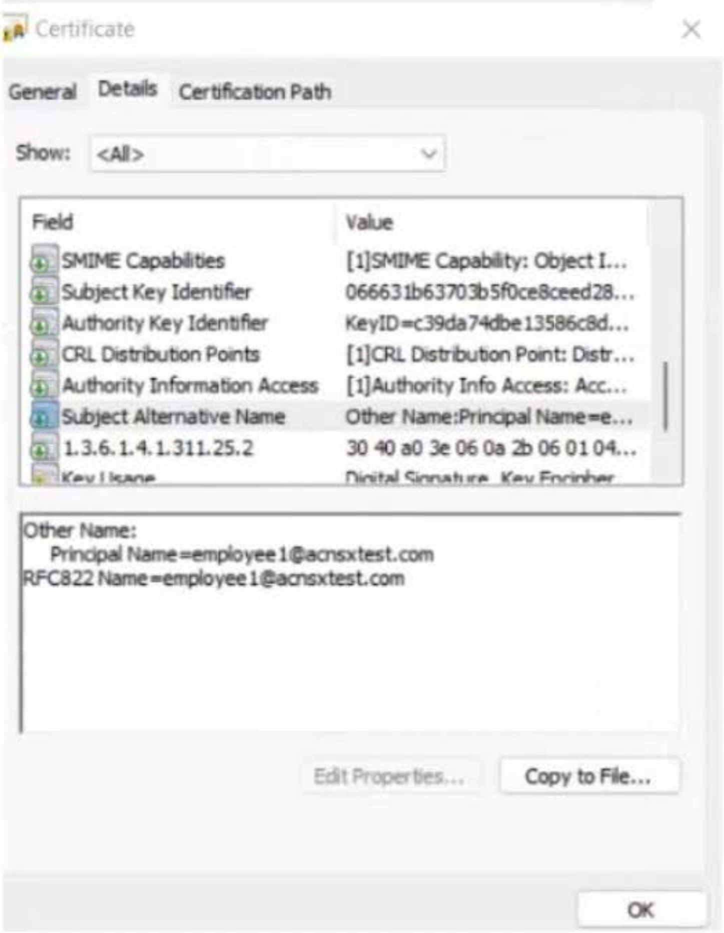
Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: employee1

Issued by: intca.acnsxtest.com

Valid from 8/12/2022 to 8/12/2023



Show: <All>

Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	066631b63703b5f0ce8ceed28...
Authority Key Identifier	KeyID=c39da74dbe13586c8d...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=e...
1.3.6.1.4.1.311.25.2	30 40 a0 3e 06 0a 2b 06 01 04...
Key Usage	Digital Signature, Key Encipher

```
Other Name:
    Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
```

The company is in the process of adding Microsoft Endpoint Manager (Intune) to manage its mobile clients. The customer is maintaining the on-prem AD for now and uses Azure AD Connect to sync with Azure AD.

# Requirements for issuing certificates to mobile clients

The company wants to use ClearPass Onboard to deploy certificates automatically to mobile clients enrolled in Intune. During this process, Onboard should communicate with Azure AD to validate the clients. High availability should also be

provided for this scenario; in other words, clients should be able to get certificates from Subscriber 2 if Subscriber 1 is down.

The Intune admins intend to create certificate profiles that include a UPN SAN with the UPN of the user who enrolled the device.

# Requirements for authenticating clients

The customer requires all types of clients to connect and authenticate on the same corporate SSID.

The company wants CPPM to use these authentication methods:

1.

EAP-TLS to authenticate users on mobile clients registered in Intune

2.

TEAR, with EAP-TLS as the inner method to authenticate Windows domain computers and the users on them To succeed, EAP-TLS (standalone or as a TEAP method) clients must meet these requirements:

1.

Their certificate is valid and is not revoked, as validated by OCSP

2.

The client\\'s username matches an account in AD # Requirements for assigning clients to roles After authentication, the customer wants the CPPM to assign clients to ClearPass roles based on the following rules:

1.

Clients with certificates issued by Onboard are assigned the "mobile-onboarded" role

2.

Clients that have passed TEAP Method 1 are assigned the "domain-computer" role

3.

Clients in the AD group "Medical" are assigned the "medical-staff" role

4.

Clients in the AD group "Reception" are assigned to the "reception-staff" role The customer requires CPPM to assign authenticated clients to AOS firewall roles as follows:

1.

Assign medical staff on mobile-onboarded clients to the "medical-mobile" firewall role

2.

Assign other mobile-onboarded clients to the "mobile-other" firewall role

3.

Assign medical staff on domain computers to the "medical-domain" firewall role

4.

All reception staff on domain computers to the "reception-domain" firewall role

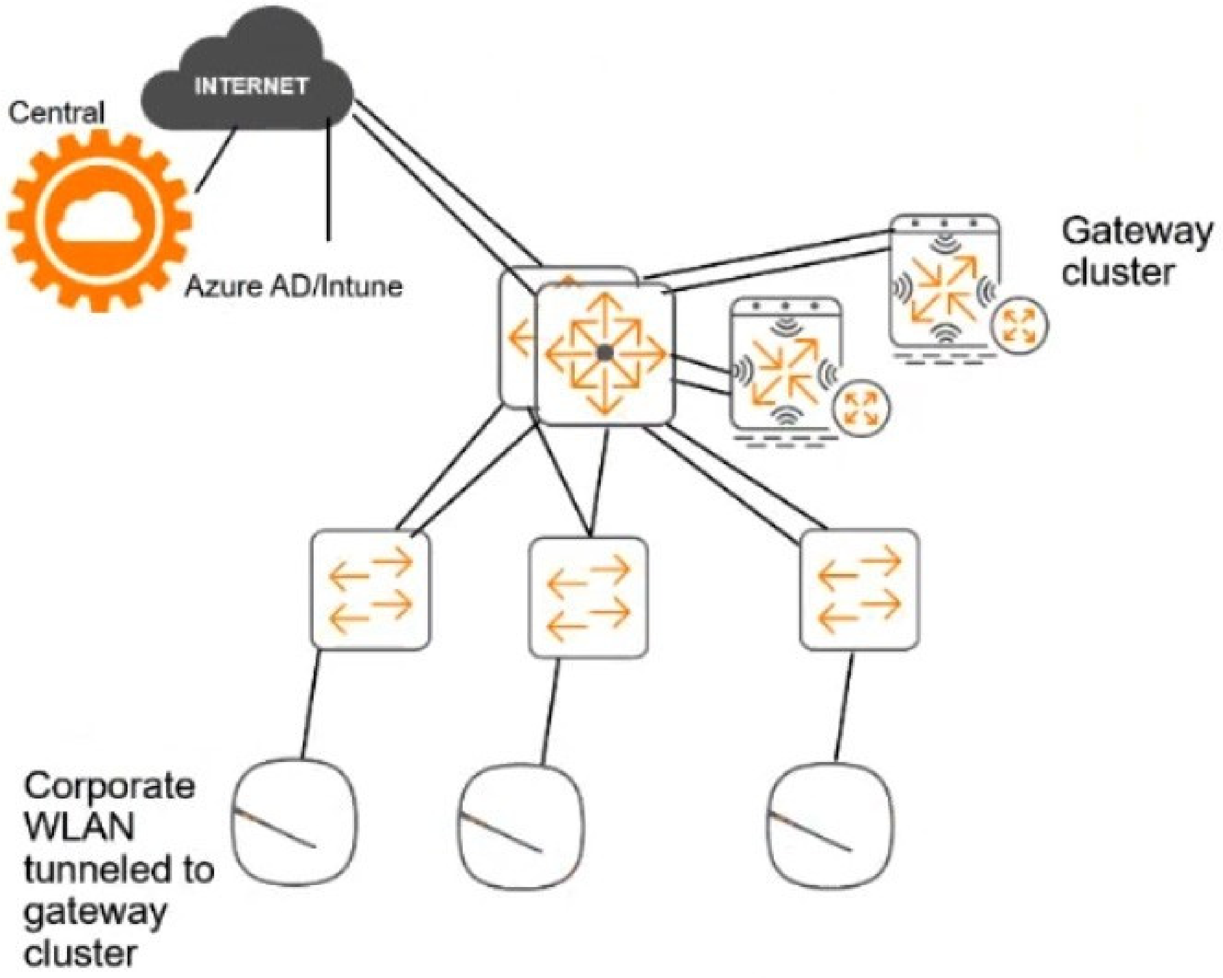
5.

All domain computers with no valid user logged in to the "computer-only" firewall role

6.

Deny other clients access # Other requirements Communications between ClearPass servers and on-prem AD domain controllers must be encrypted. # Network topology For the network infrastructure, this customer has Aruba APs and Aruba gateways, which are managed by Central. APs use tunneled WLANs, which tunnel traffic to the gateway cluster. The customer also has AOS-CX switches that are not

managed by Central at this point.



# ClearPass cluster IP addressing and hostnames

A customer\\'s ClearPass cluster has these IP addresses:

1.

Publisher = 10.47.47.5

2.

Subscriber 1 = 10.47.47.6

3.

Subscriber 2 = 10.47.47.7

4.

Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8

The customer\\'s DNS server has these entries

1.

cp.acnsxtest.com = 10.47.47.5

2.

cps1.acnsxtest.com = 10.47.47.6

3.

cps2.acnsxtest.com = 10.47.47.7

4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

The customer needs a secure way for users to enroll their new wireless clients in Intune. You are recommending a new WLAN that will provide the users with limited access for the enrollment.

You have set up captive portal for clients on this WLAN to a web page with instructions for enrolling devices. You will need to add several hostnames to the captive portal allowlist manually.

What is one of those hostnames?

A. The hostname used by ClearPass Policy ManaGer\\'s RADIUS services

B. The ClearPass Onboard hostname referenced in an Onboard provisioninG profile

C. The ClearPass Onboard hostname referenced in Intune SCEP profiles

D. The hostname used by the on-prem domain controllers

Correct Answer: B